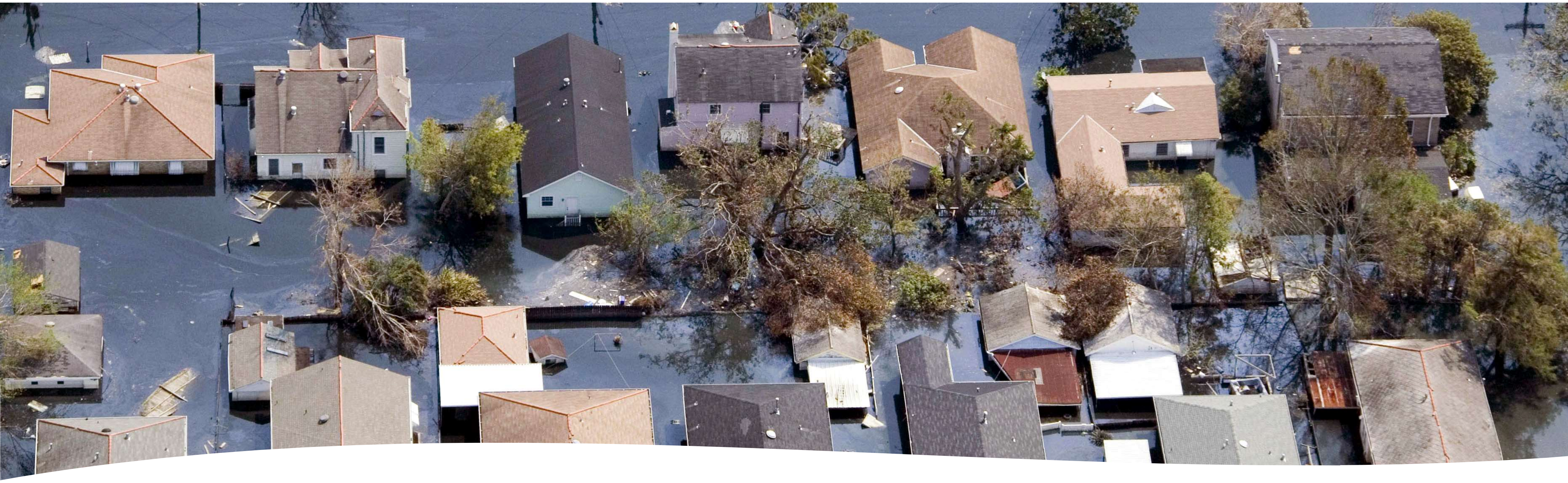
Vulnerabilities, Threats, and Controls

Dr. Bhaskar Mondal

Vulnerabilities, Threats, and Controls

- **Vulnerability:** a weakness in a security system
- **Threat:** circumstances that have a *potential* to cause harm
- **Controls**: means and ways to block a threat, which tries to exploit one or more vulnerabilities

[Pfleeger & Pfleeger]



Vulnerabilities, Threats, and Controls

- Example - New Orleans disaster (Hurricane Katrina)
  - Q: What were city vulnerabilities, threats, and controls?
  - A: **Vulnerabilities**: location below water level, geographical location in hurricane area, …

    Threats: hurricane, dam damage, terrorist attack, …

    Controls: dams and other civil infrastructures, emergency response plan, …

Attacks

Attack

- Attack (materialization of a vulnerability/threat combination)
  - exploitation of one or more vulnerabilities by a threat; tries to defeat controls
- Attack may be:
  - *Successful* (a.k.a. an *exploit*)
    - resulting in a breach of security, a system penetration, etc.
  - *Unsuccessful*
    - when controls block a threat trying to exploit a vulnerability

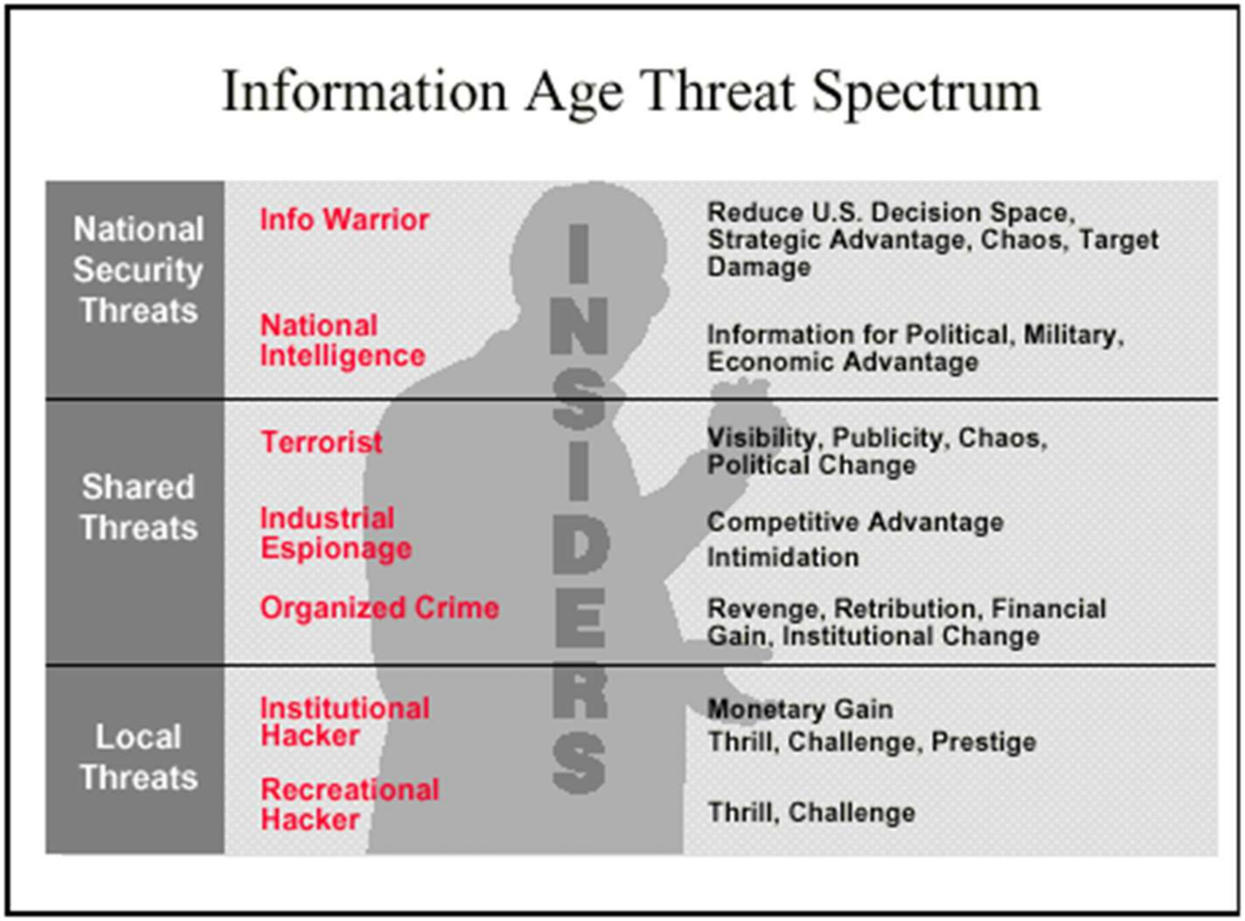
[Pfleeger & Pfleeger]

Security Threats

Dr. Bhaskar Mondal

Threat Spectrum

> *"A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems…relies entirely on computer networks."*—***Foreign Government Newspaper***



Information Age Threat Spectrum

National Security Threats	Info Warrior	Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threats	Terrorist	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage Intimidation
	Organized Crime	Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	Institutional Hacker	Monetary Gain Thrill, Challenge, Prestige
	Recreational Hacker	Thrill, Challenge

- Local threats
  - Recreational hackers
  - Institutional hackers
- Shared threats
  - Organized crime
  - Industrial espionage
  - Terrorism
- National security threats
  - National intelligence
  - Info warriors

Kinds of Threats

Interception/ Disclosure

- an unauthorized party (human or not) gains access to an asset
- Snooping: the unauthorized interception of information

Interruption/ Disruption

- an asset becomes lost, unavailable, or unusable.
- prevention of correct operation;
- Denial of Service (DOS) attack

Modification

- an unauthorized party changes the state of an asset.
- Masquerading or spoofing (an impersonation of one entity by another)

Fabrication

- an unauthorized party counterfeits an asset
- inserts fake objects into the system

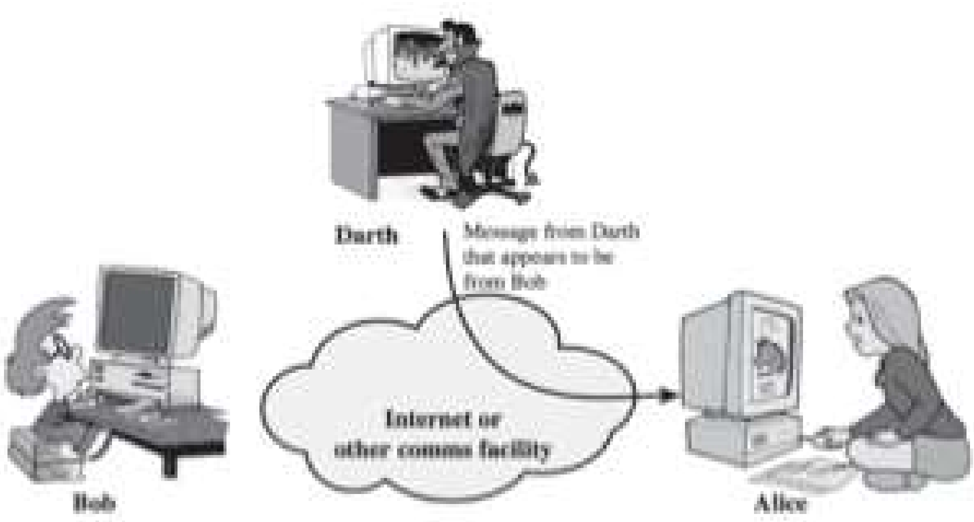

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

Figure 1.7 Masquerade

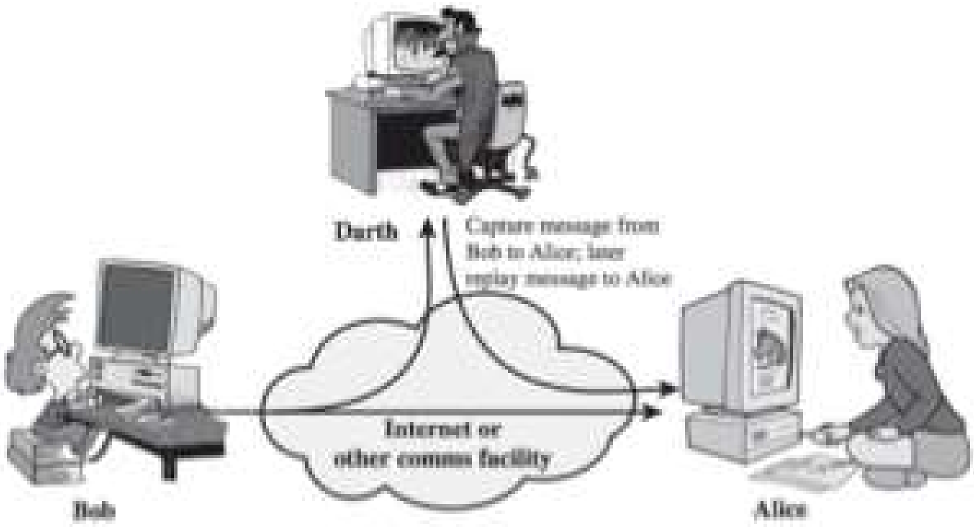
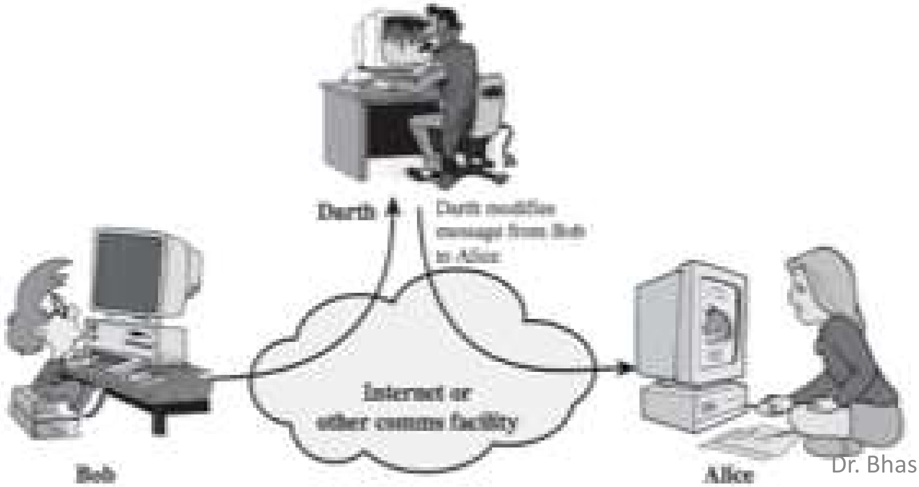
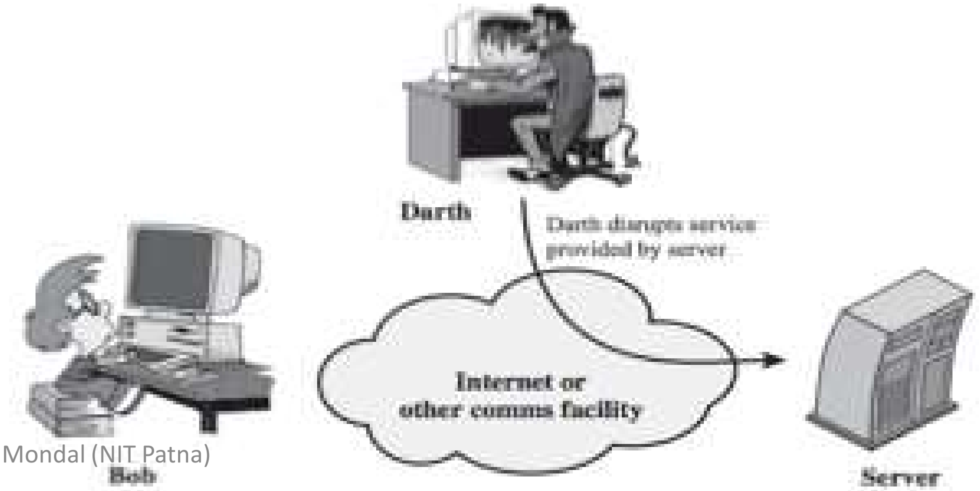
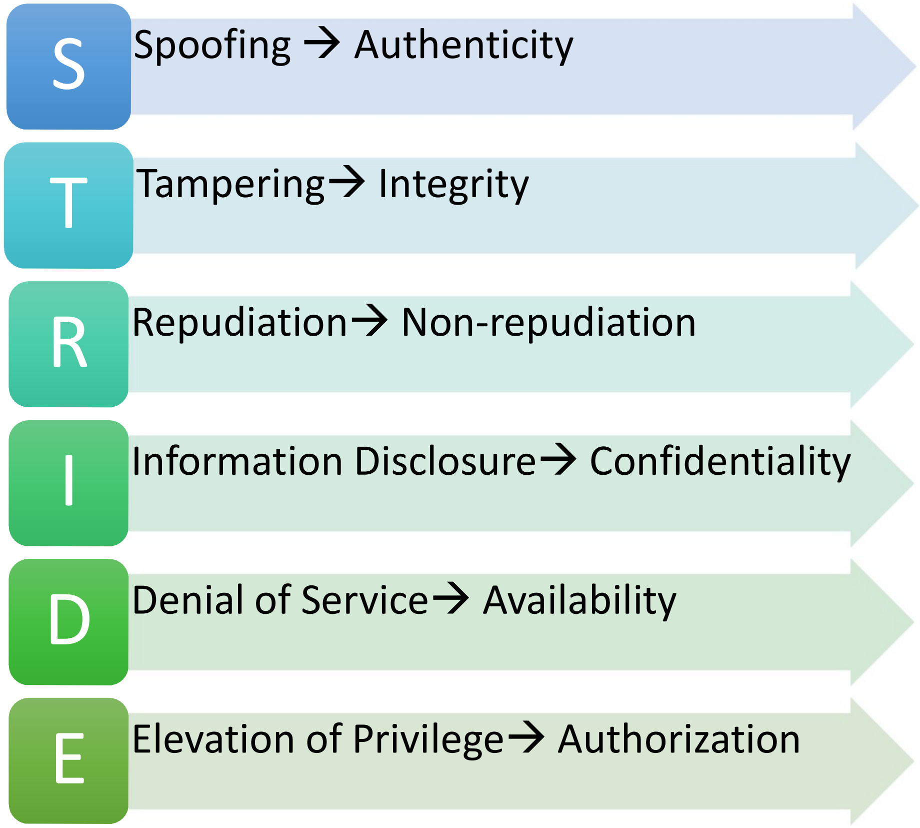

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Figure 1.7 Replay


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

The S.T.R.I.D.E. model of threats



S Spoofing → Authenticity

T Tampering→ Integrity

R Repudiation→ Non-repudiation

I Information Disclosure→ Confidentiality

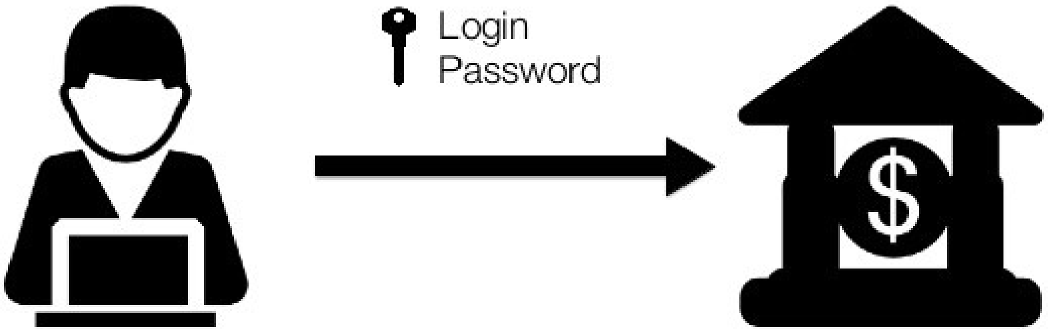
D Denial of Service→ Availability

E Elevation of Privilege→ Authorization

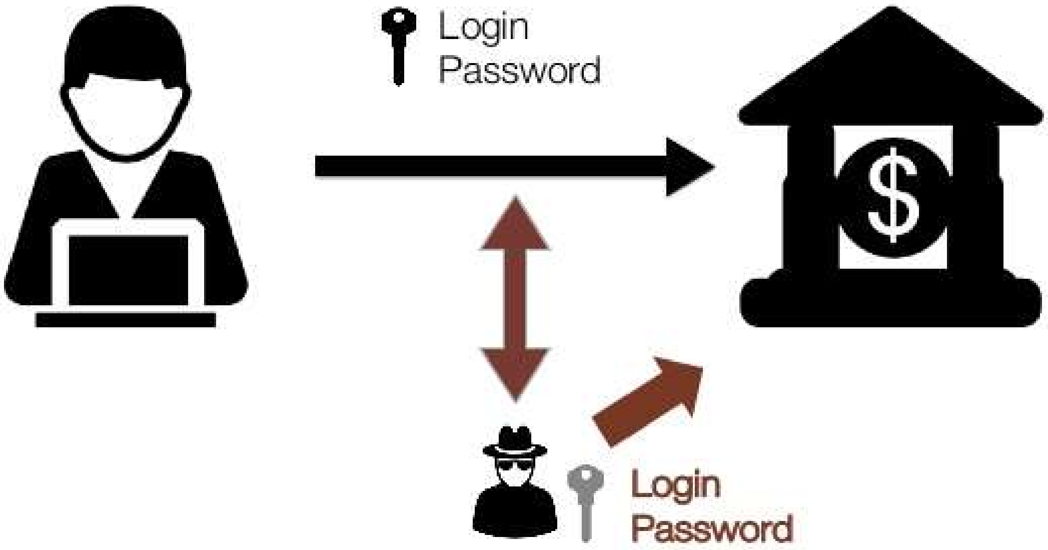
Spoofing

The attacker steals your identity

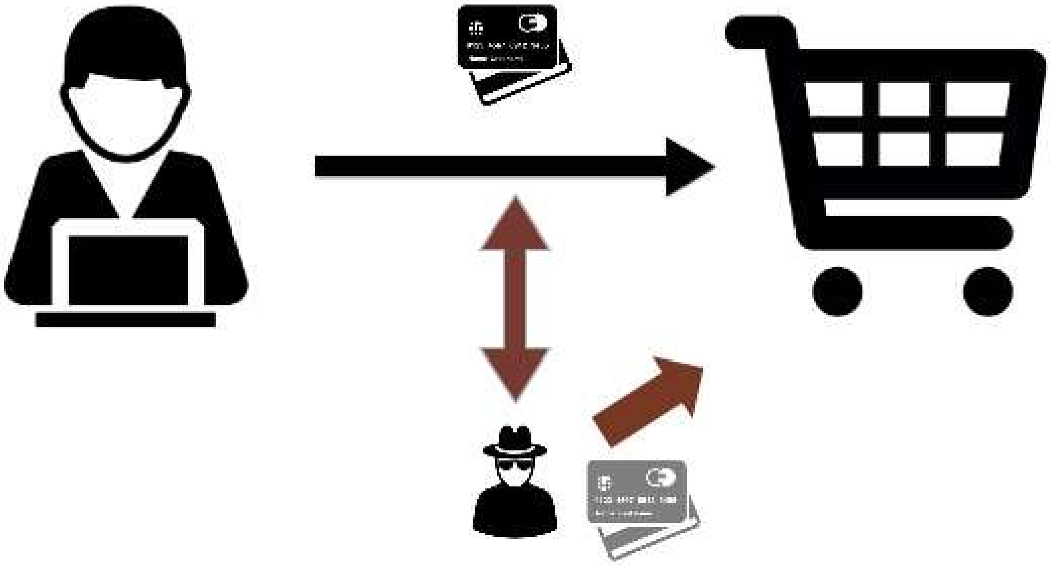
Spoofing



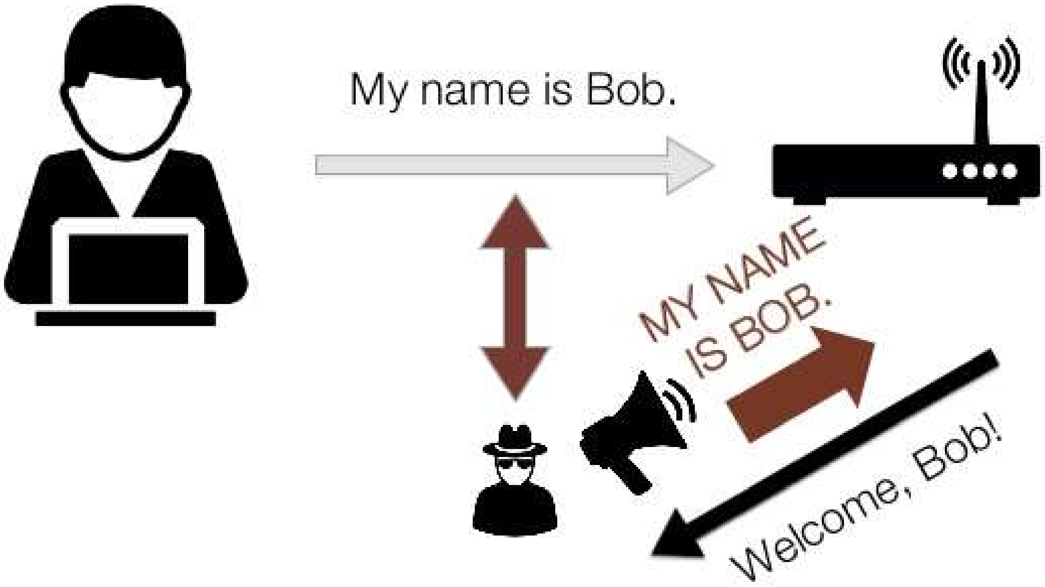
Spoofing



Spoofing



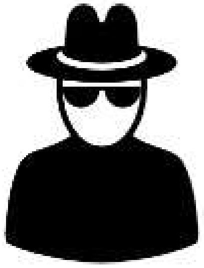
Spoofing



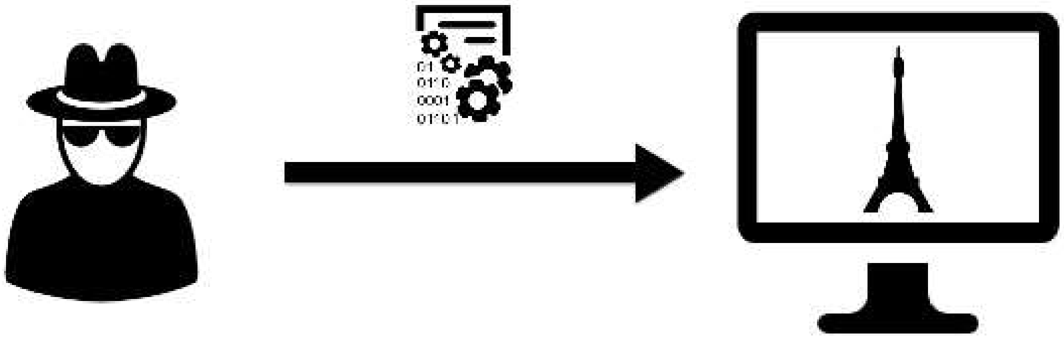
Tampering

The attacker alters your data

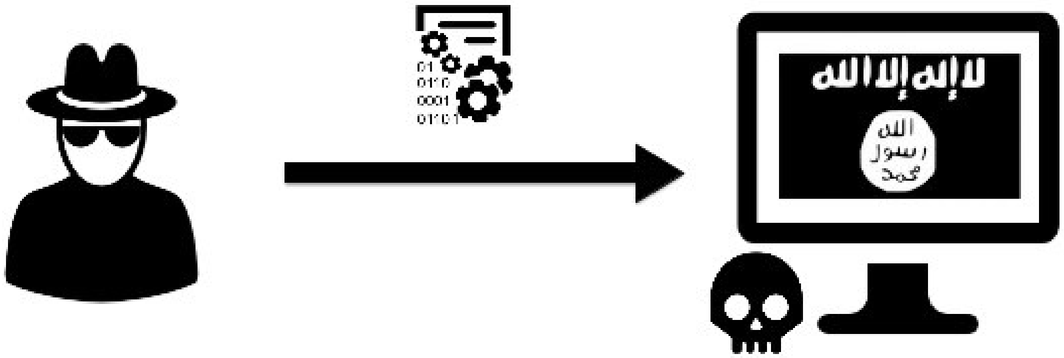
Tampering



Tampering



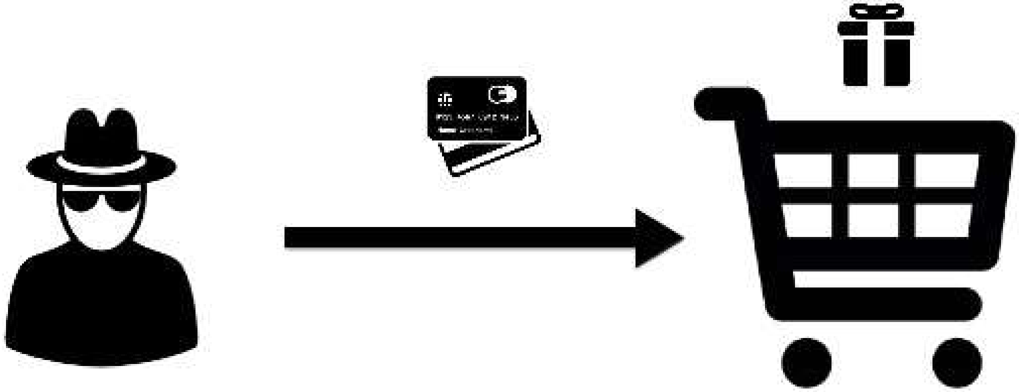
Tampering



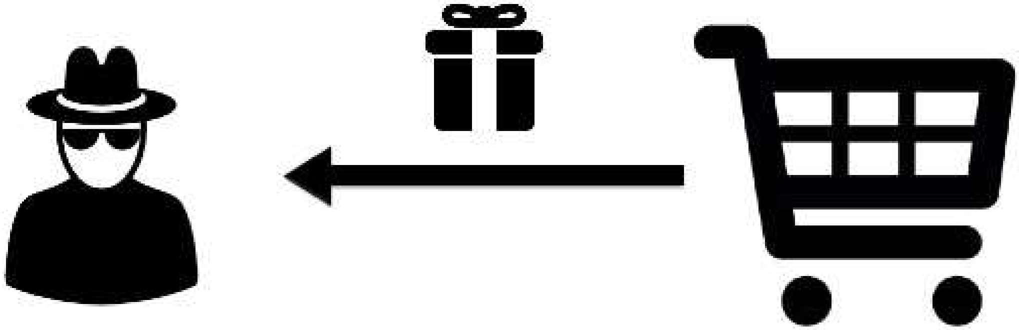
Repudiation

The attacker makes your system believe a transaction never happened

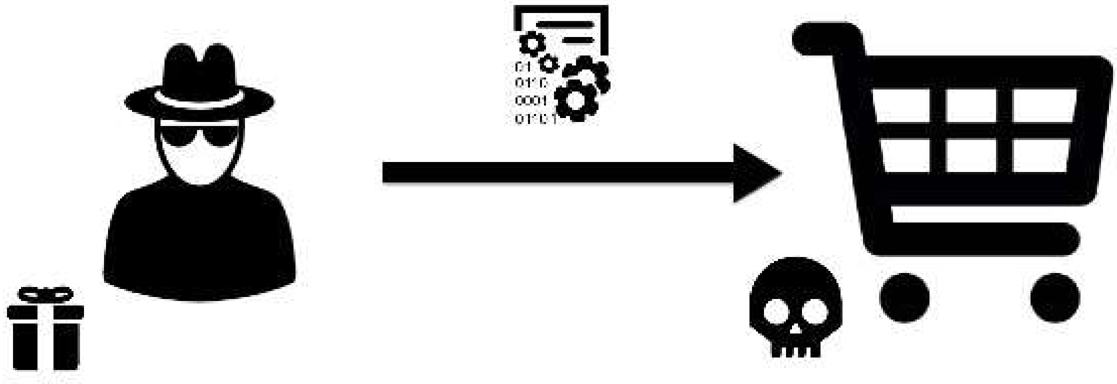
Repudiation



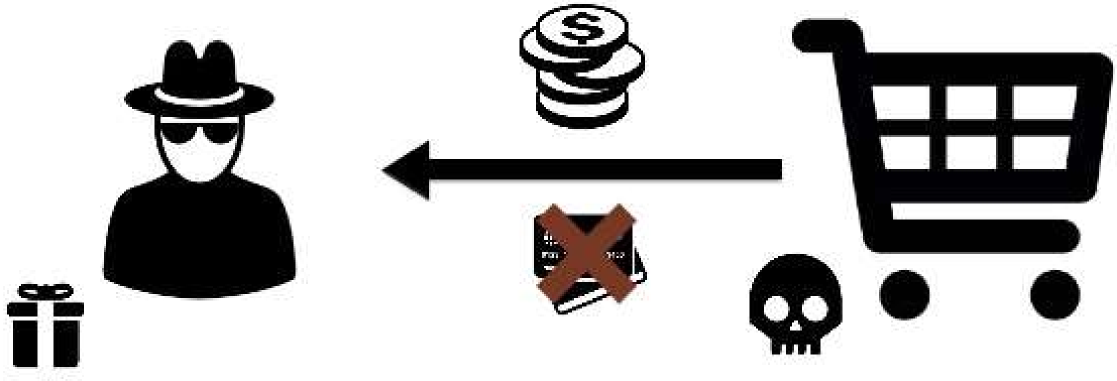
Repudiation



Repudiation



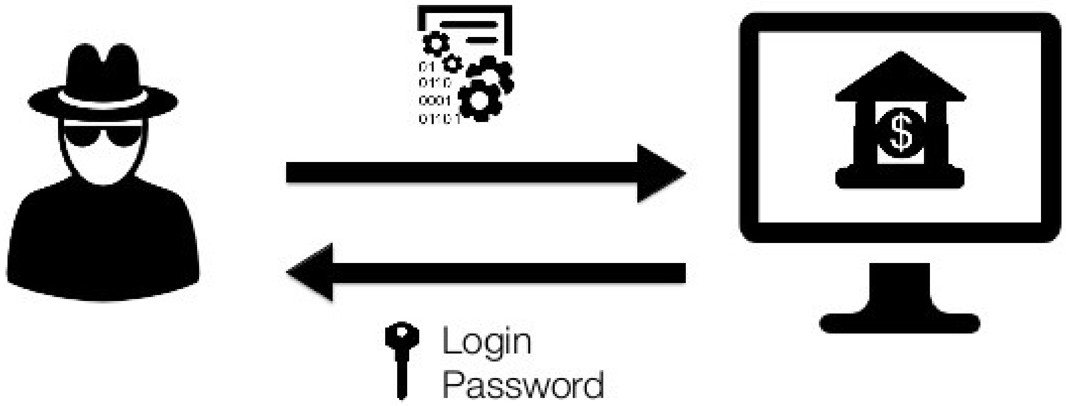
Repudiation



Information Disclosure

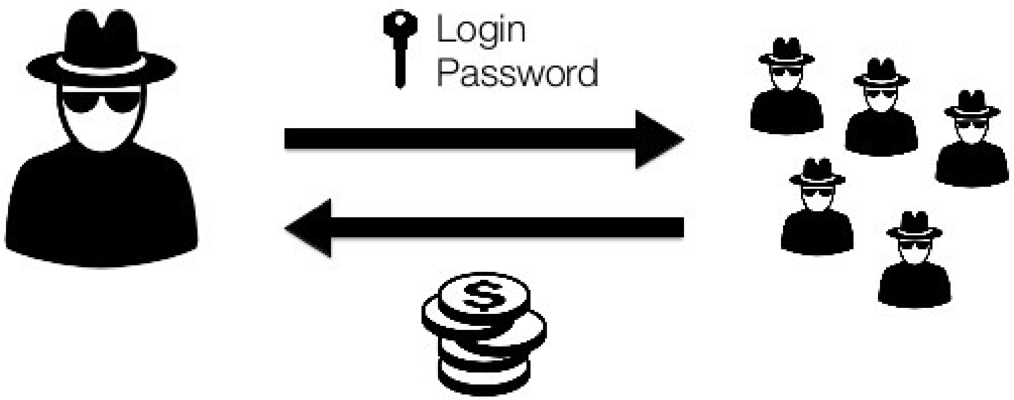
The attacker publishes confidential information

Information Disclosure



Login
Password

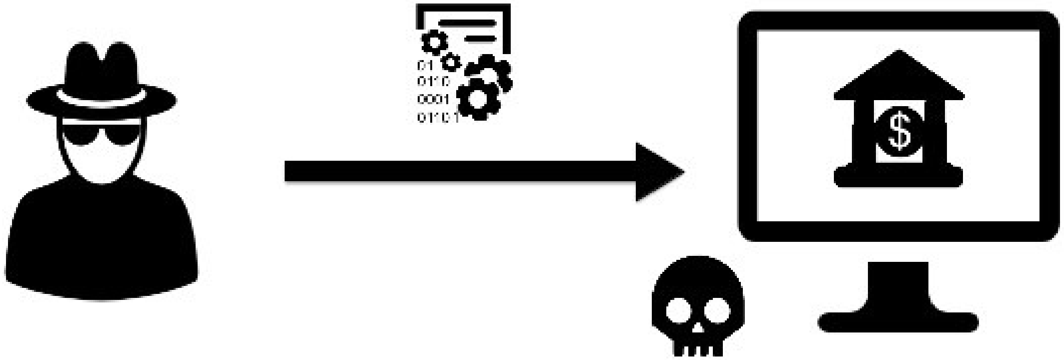
Information Disclosure



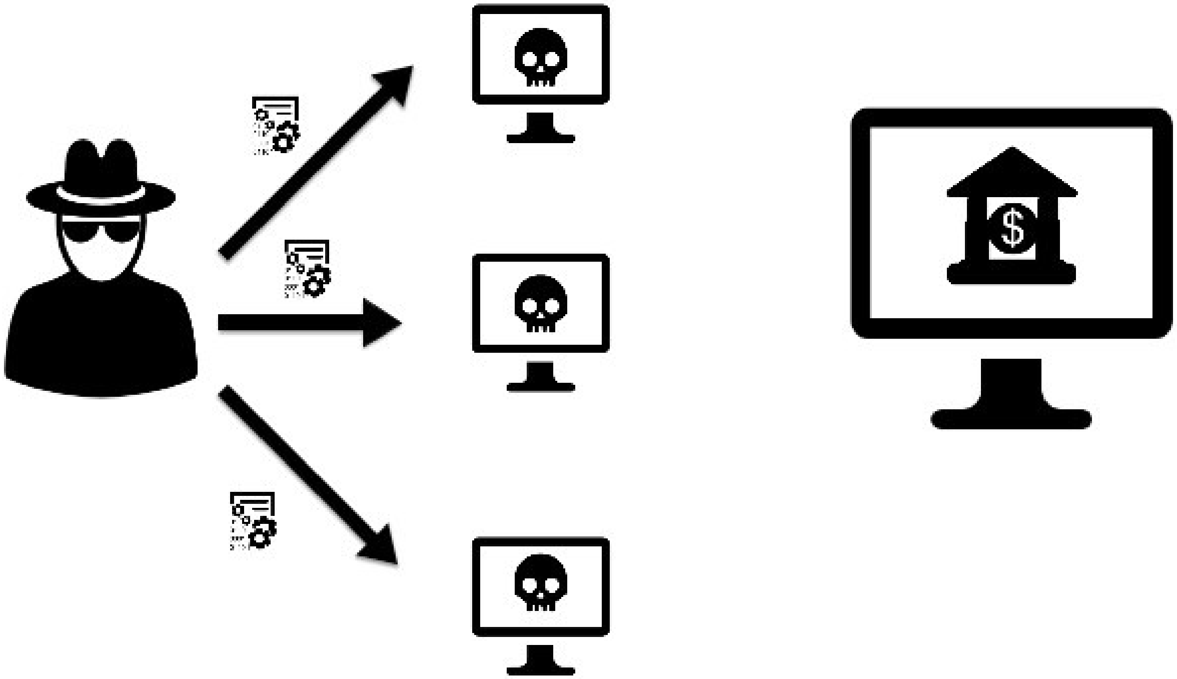
Denial of Service

The attacker makes a system unavailabl

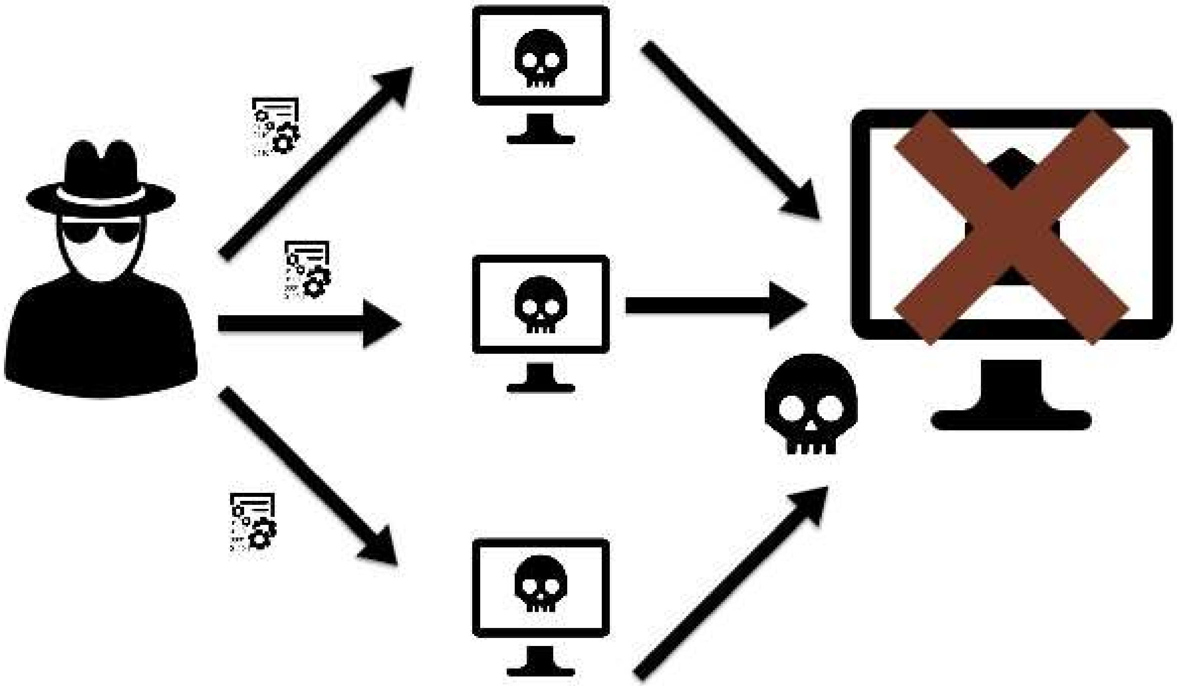
Denial of Service



Distributed Denial of Service



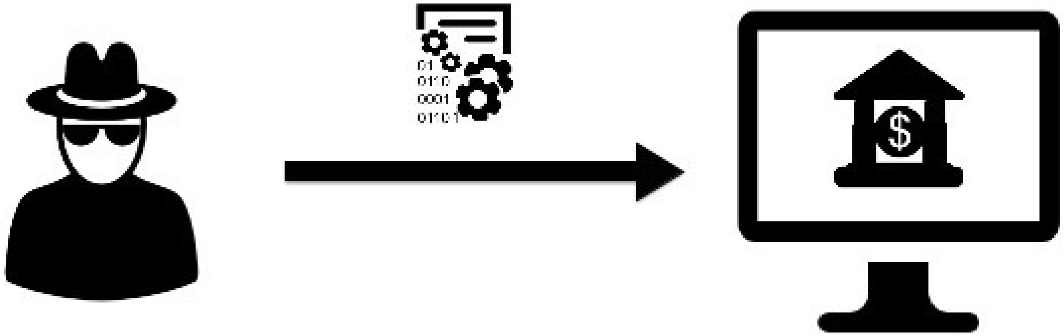
Distributed Denial of Service



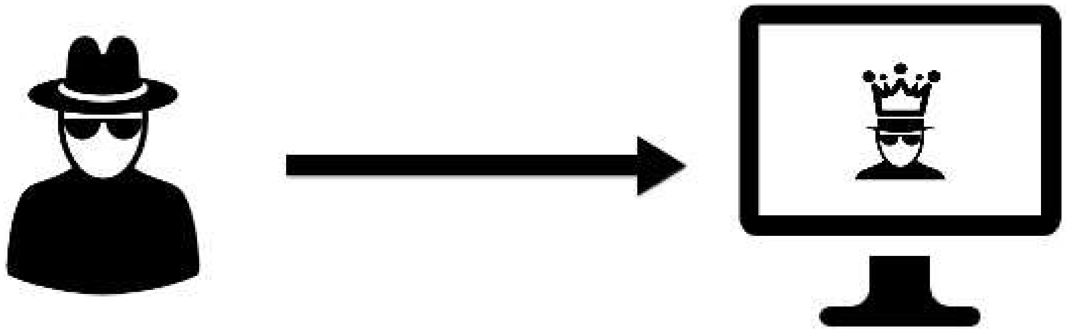
Elevation of Privilege

(Privilege Escalation) The attacker gets administrator rights on the system.

Elevation of Privilege (Privilege Escalation)



Elevation of Privilege (Privilege Escalation)



Threats are multiple, and so are vectors.

Hardware security
Network security
Software security
Social engineering
…